6.6.2 Passenger Rail / Public Transit

Passenger rail/public transit includes multiple-occupancy vehicles designed to transport customers on regional and local routes. Passenger rail/public transit vehicles include transit buses, trolleybuses, monorails, light rail, subways, commuter rails, long-distance rails, automated guide-way transit, inclined planes, and cable cars.[23] Each of these vehicle types has associated passenger and support facilities, which in turn will have associated control systems.

Passenger Rail / Public Transit Vehicles and Systems

Transit buses, also known as commuter buses, city buses, or public buses, are buses used for short-distance public transport purposes.

Trolleybuses are electric buses that draw their electricity from overhead wires (generally suspended from roadside posts) using spring-loaded trolley poles. Two wires and poles are required to complete the electrical circuit.

Light rail is a term used to refer to rail systems with rapid transit-style features that usually use electric rail cars operating mostly in private rights-of-way separated from other traffic. Light rail generally has lower capacity and slower speed than heavy rail and metro systems, but higher capacity and faster speed than street-running tram systems.

Monorails are rail-based transportation systems based on a single rail, which acts as its sole support and guideway.

Subways are rapid transit electric passenger railways located in urban areas with high capacity and frequency and grade separation from other traffic. Subways are typically located either in underground tunnels or on elevated rails above street level.

Commuter rails are passenger rail transport services that primarily operate between a city center and the middle to outer suburbs and commuter towns or other locations that draw large numbers of people who -travel on a daily basis.

Long-distance rails travel between many cities and/or regions of a country, and sometimes cross several countries. They often have a dining or restaurant car to allow passengers to have a meal during the course of their journey.

Automated guide-way transit systems are fully automated, driverless, grade-separated transit systems in which vehicles automatically travel along a guideway.

Inclined planes are straight ramps cut into a hillside and used for moving loads up and down the hill. Inclined planes are often provided with cars riding on rails and pulled up and lowered down using a cable drive system powered by a steam engine.

Cable cars are a variety of transportation systems relying on cables to pull vehicles along or lower then at a steady state, or a vehicle on these systems.

Source: Wikipedia

---

[23] DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan*, 2010, Table 1-1.

Figure 14: Underground Subway[24]

Because passenger rail/public transit includes a wide variety of vehicles and equipment travelling over dedicated pathways, central control and monitoring of all aspects of the transit network is critical to maintaining operational control in this mode. Control systems in passenger rail/public transit can be described both by their common designations and by the functions they perform. Some control systems provide a specific function (e.g., train control), whereas others integrate different functions (e.g., emergency alarms, fire detection, gas monitoring) into one or more enhanced systems. Passenger rail/public transit control systems can be grouped into the following six main system types:[25]

- **Control systems** include train control systems and SCADA systems. Train control systems are used to operate underground and surface public transit vehicles. These systems may operate in either a semi-autonomous mode (used for underground travel) or a speed limited manual mode (when traveling on streets and other aboveground surfaces). They include equipment in the trains and buses as well as along the route (e.g., traffic lights, gates, etc.). SCADA systems control the supply of power to transit stations (used to operate building management aspects such as fire life safety, HVAC, intrusion detection, etc., equipment) and to move the actual passenger trains. Such systems often link each transit station to others along the transit route, and provide remote control and monitoring of associated field equipment.

[24] Source: Volpe project photograph.
[25] APTA, *Draft Technical Recommended Practice for Securing Control and Communications Systems in Transit Environments: Part 1 - Elements, Organization and Risk Assessment/Management*, Version 1.0.9, August 31, 2009.

- **Communication systems** include radio, closed circuit television (CCTV), intercom, public information displays, and public address systems used to provide transit passenger with transportation information such as estimated arrival time, delays, emergency directives, etc.

- **Security control systems** include CCTV, intrusion detection, video surveillance, alarm, and other monitoring systems designed to provide real-time views of the various system assets such as platforms, station lobbies, etc. These systems are usually connected to an operations center, where recorded information is monitored and stored.

Figure 15: Passenger Access Control Gates at a Subway[26]

- **Data transmission systems** include fiber optic networks, copper networks, leased lines, and wireless network systems that provide the data communications infrastructure between a transit agency's control center and other transit buildings and properties and for local area networks (LANs) and wide area networks (WANs).

- **Fare collection systems** are used to collect transit payments from fare collection devices at each station. Fare collection systems can often support point-of-sale devices situated in locations not directly controlled by the transit authority and wireless fare card verification devices located throughout the transit system. These systems are often integrated with entry/exit gates, station access points/garages, etc., and are frequently linked with financial systems and the governing transit agency's back office functions.

[26] Source: Volpe project photograph.

- **Vehicle monitoring systems** refer to control systems, similar to those for train control, used for automatic vehicle monitoring of buses, streetcars, and other surface systems, including non-revenue equipment.

Many public transit agencies provide more than one transportation mode and when they do, each mode is operated practically autonomously. In addition, passenger rail/public transit has a variety of other cybersecurity challenges, including:

Different Control Systems. Control systems may be completely different. For example, bus operations will typically have GPS-based automated vehicle location systems which simply "track" bus movement whereas rail will have various means of controlling track switches and sometimes include automatic functions to control train power, routing, and speed.

Separate Network and Communications Teams. The business/management division and the modes often have their own network and communications engineers. For example, the business/management division may have a dedicated IT staff to manage the IT network and workstations while each mode may have its own control system engineers to build its own networks to support its control systems. These separate teams can result in different security practices and standards being implemented for networks and communications.

Shared Communications Backbone. To tie together the different modes, a shared network and communications backbone is often used. This backbone is often deployed and managed by rail control systems engineers to support the train control systems, but the entire agency may use the backbones as the core of its WAN. Such a scenario results in networks and control systems with different security practices and standards operating on the same WAN.

Legacy Control Systems on Modern Networks and Being Replaced by IP-Based Control Systems. Most transit agencies have already used modems to convert legacy analog control signals to digital signals to take advantage of WANs and to extend the reach of their controllers. Many agencies are also making incremental upgrades to their control systems by replacing legacy analog controllers with digital and IP-based controllers. Public transportation is replacing its legacy control systems, often isolated from other industry systems, with next generation control systems based on traditional IT technologies that rely on networks, wireless communications, GPS, and microprocessor-based devices. While there are many benefits to these practices, an unintended consequence is that systems previously immune to cyber vulnerabilities are now vulnerable to cybersecurity attacks.

IP-Based Security Systems Driving the Design of Agency WANs. Physical safety and security are vital to transit agencies and most have or are deploying agency-wide security measures including IP-based access control systems and IP-based video surveillance. These security systems are driving the design of WANs and significantly increasing the number of IP-based edge devices on transit agency networks.

7.0 Goals, Objectives, Metrics and Milestones

This section presents four strategic goals designed to assist transportation professionals in focusing activities and resources for improving the cybersecurity of ICS. These goals provide a logical framework for organizing the collective efforts of the transportation industry, government, and other key stakeholders for achieving ICS cybersecurity. The goals are broad-based, applicable to all transportation modes and organizations, developed around a 10-year outlook, and designed to be achieved concurrently. When viewed together, the four goals are intended to capture the full spectrum of activities needed for transportation control systems cybersecurity.

Near-term (0-2 years), mid-term (2-5 years), and long-term (5-10 years) objectives, with corresponding milestones and metrics (i.e., Near-Term Objective “a” matches with Near-Term Milestone and Metric “a”)[27], are presented for each goal. This information gives organizations specific activities to conduct to better secure transportation ICSs, and provides corresponding milestones and metrics for individual organizations to use for determining whether they have achieved the objective. Because this Transportation Roadmap is developed to be applicable to the whole Transportation Sector as well as to individual modes and organizations, the milestones and metrics also provide broad quantification information each mode, and the Transportation Sector, can use to determine the mode’s/Sector’s progress as a whole towards achieving the corresponding objective.

The four Transportation Roadmap goals, and their corresponding end states, are:

Goal 1: Build a Culture of Cybersecurity
End State: Cybersecurity and ICS are viewed as inseparable and integrated throughout the Transportation Sector.

Goal 2: Assess and Monitor Risk
End State: The Transportation Sector has a robust portfolio of ICS-recommended security analysis tools to effectively assess and monitor ICS cybersecurity risk.

Goal 3: Develop and Implement Risk Reduction and Mitigation Measures
End State: Security solutions for legacy systems, new architectural designs, and secured communication systems in the Transportation Sector are readily available and deployed across the Sector.

Goal 4: Manage Incidents
End State: The Transportation Sector is quickly alerted of cybersecurity ICS incidents, and sophisticated, effective, and efficient mitigation strategies are implemented and in operation.

[27] While Objectives within each timeframe (Near-, Mid-, and Long-Term) match to the corresponding Milestone and Metric in the same timeframe, Objectives (and thus Milestones and Metrics) between timeframes are not designed to match (e.g., Mid-Term Objective “a” is not intended to match with Near- and Long-Term Objective “a”).

The information presented in this section should be viewed as a starting point for enhancing transportation ICS cybersecurity; as each organization, transportation mode, and the Transportation Sector itself improves its cybersecurity posture, new objectives, milestones, and metrics should be developed based on the current cybersecurity threats and risks. Similarly, this information can be used by individual transportation modes and organizations to develop modal and organization-specific roadmaps for securing ICSs.

Goal 1: Build a Culture of Cybersecurity

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Develop and implement an ICS cybersecurity governance model. b. Identify roles and responsibilities, structure, and authorities for ICS cybersecurity planning and risk management. c. Educate transportation executives on the importance of ICS cybersecurity. d. Establish ICS cybersecurity policies and procedures, resources, and budget/funding. e. Develop a cybersecurity awareness training program, and begin delivering it to new hires and existing employees.	a. The organization has a documented ICS cybersecurity business case. b. Personnel have been formally assigned ICS cybersecurity planning and risk management responsibilities and budgets. c. Many transportation executives recognize ICS cybersecurity as mission critical. d. The organization has identified the ICS policies and procedures it will follow, and has established the necessary ICS resources and budget/funding. e. A formal cybersecurity awareness program is developed, and the organization has begun to deliver the training to its employees.
Mid-Term (2-5 years)	a. Refine the cybersecurity awareness training program by increasing the depth of information provided and the extent of employees trained. b. Institutionalize cybersecurity language/methodologies in ICS contracts, user agreements, statements of work, asset management procedures, etc. c. Develop a robust ICS self-assessment program/business case. d. Develop security assessment capabilities for new and legacy ICSs. e. Establish a mechanism that allows for frequent and ongoing collaboration between operations and security cyber staff and ICS operators and engineers.	a. The organization has further developed its cybersecurity awareness training program, and has provided the training to many of its employees. b. Most ICS-related procurements, documents, procedures, and policies include provisions for cybersecurity. c. Asset owners and operators perform self-assessments of most of their ICSs according to the frequency identified in their associated program/business case. d. The organization identifies its current security assessment capabilities for new and legacy ICSs, including the types of assessment tools utilized. e. The organization has established a formal means for periodic collaboration between operations and security cyber staff and ICS operators and engineers.
Long-Term (5-10 years)	a. Establish automated processes to secure ICSs. b. Ensure that cybersecurity awareness training is periodically updated and provided to personnel at all organizational levels. c. Incorporate cybersecurity language, reviews, and considerations into all levels of ICS-related business practices and budgetary considerations. d. Establish ISACs (or equivalent) for each transportation mode and for the Transportation Sector.	a. Most ICSs are continuously monitored via established automated processes. b. The organization has an established process for updating its cybersecurity awareness training, with most staff receiving annual cybersecurity awareness refresher training. c. Cybersecurity is integrated into most ICS business practices. d. Modal ISACs, together with a Transportation Sector ISAC (or equivalent), serve as the conduit of cross-modal lessons learned and best practices in ICS cybersecurity, and provide a forum for partnership, outreach, and information sharing within each mode and throughout the Transportation Sector.
End State:	**Cybersecurity and ICS are viewed as inseparable and integrated throughout the Transportation Sector.**	

Goal 2: Assess and Monitor Risk

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Identify risk management framework and standards. b. Identify common metrics for benchmarking ICS risk (threats-vulnerabilities-consequences). c. Integrate cybersecurity into business functions and operation plans. d. Develop and disseminate ICS risk assessment and reporting standards and guidelines that enable cybersecurity tools and metrics to be effectively deployed. e. Identify cybersecurity risk management roles and responsibilities, including establishing authorities responsible for accepting and mitigating cybersecurity risk. f. Adopt and deploy cybersecurity posture assessment tools (Cybersecurity Evaluation Tool (CSET) or equivalent) for ICS cybersecurity vulnerability assessments.	a. Each organization identifies the risk management framework and standards it will follow. b. Each organization prioritizes its identified ICS cybersecurity risks based on defined common metrics. c. All business functions and operation plans contain a cybersecurity component. d. ICS risk assessment and reporting guidelines are published and disseminated throughout each organization. e. All asset owners and operators have identified personnel responsible for ICS cybersecurity risk management. f. Many asset owners and operators have deployed cybersecurity posture assessment tools (CSET or equivalent).
Mid-Term (2-5 years)	a. Develop and implement a risk management model and strategy. b. Develop and implement a risk assessment program, with considerations for both top-down and bottom-up approaches. c. Examine and test the use of automated tool options for ICSs. d. Examine and assess real-time security assessment capabilities for new and, where appropriate, legacy systems. e. Develop and implement a cyber risk management training program for personnel with cybersecurity responsibilities.	a. Each organization identifies the risk management model and strategy it will use. b. Most asset owners and operators have implemented a cybersecurity ICS risk assessment program, with considerations for both top-down and bottom-up approaches. c. Most owners and operator have examined and tested the use of automated tool options for ICSs. d. Real-time security assessment capabilities have been reviewed for most ICSs (new and legacy). e. Many employees with ICS responsibilities receive specialized cybersecurity training that includes instruction on risk assessment tools aligned with the organization's risk management model, strategy, framework, and standards.
Long-Term (5-10 years)	a. Establish a formal risk management program. b. Establish and implement a continuous and automated risk monitoring program, including tools, for ICSs. c. Incorporate risk management considerations into all levels of ICS cybersecurity (contracts, user agreements, purchases, etc.). d. Establish, and regularly use, communication mechanisms for measuring risk management performance and benchmarking among the transportation modes and with other sectors. e. Develop and implement a cybersecurity ICS training program review process.	a. Each organization has established a formal risk management program, including related processes, for risk measurement and reporting. b. Most asset owners and operators are using continuous and automated ICS risk monitoring programs and tools. c. Cybersecurity is integrated into most ICS business practices. d. Each transportation mode has an active program for ICS security profile assessment, and regularly shares this information, for benchmarking purposes, with other modes and sectors. e. Each organization has established and implemented a review process for monitoring its cybersecurity ICS training program.
End State:	**The Transportation Sector has a robust portfolio of ICS-recommended security analysis tools to effectively assess and monitor ICS cybersecurity risk.**	

Goal 3: Develop and Implement Risk Reduction and Mitigation Measures

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Develop and disseminate ICS protection guidelines that assist in ensuring existing access controls are properly implemented and enabled. b. Develop a template protocol for responding to cyber incidents. c. Establish mechanisms for sharing information between asset owners, operators, and vendors to develop improved protection tools. d. Identify, implement, and maintain, where appropriate, existing built-in cybersecurity features in ICS equipment. e. Encourage/prioritize that ICS vendors begin implementing or improving their equipment's cybersecurity features. f. Develop, implement, and maintain cybersecurity measures—including items such as firewalls, intrusion detection, passcodes, anti-virus protection, and patching technologies—having minimum host impact and without compromising safety. g. Train employees on the ICS protection guidelines. h. Analyze the organization's current cybersecurity posture with respect to its compatibility with existing and new technologies.	a. ICS protection guidelines have been developed and disseminated throughout the organization. b. Many asset owners and operators have developed and implemented cyber incident response protocols. c. Each organization has established a process for sharing cybersecurity protection information among asset owners, operators, and vendors. d. Most asset owners and operators have identified cybersecurity features built into their control systems, and many have implemented these features, where appropriate. e. Each organization has established a preference for vendors offering equipment with enhanced cybersecurity features. f. Some asset owners and operators have begun implementing enhanced cybersecurity measures. g. Most organizations have trained their employees on their ICS protection guidelines. h. Each organization has conducted an analysis of its current cybersecurity posture, while considering compatibility with existing and new technologies.
Mid-Term (2-5 years)	a. Reduce time required for ICS patch installation. b. Develop provisions for accommodating restarts in control systems design. c. Implement and maintain effective ICS cybersecurity protection tools. d. Secure most of the interfaces between ICS and internal and external systems. e. Develop and implement specialized cybersecurity training for operators to support the proper use of, and protocols for using, the protection tools to secure ICSs. f. Perform nondisruptive intrusion tests on ICSs to demonstrate the effectiveness of automated isolation and response mechanisms.	a. Each organization has reduced its average patch installation time. b. Each organization has established provisions for accommodating control system restarts at the design level. c. Each organization has implemented and is maintaining effective cybersecurity protection tools for ICSs. d. Asset owners and operators have established secure interfaces between most ICSs and internal and external systems. e. Many operators have completed a cybersecurity training program that includes information on the protection tools and features used to secure ICSs. f. Many asset owners and operators have performed nondisruptive ICS intrusion tests.
Long-Term (5-10 years)	a. Plan for and integrate cyber-resilient ICS architectures and infrastructure that have built-in, self-defending security, and use and maintain systems and components that are secured-by-design. b. Identify best practices for connecting ICSs and business networks. c. Secure all of the interfaces between ICSs and internal and external systems. d. Ensure that most operators receive specialized cybersecurity training commensurate with their respective duties and responsibilities. e. Encourage/prioritize that real-time monitoring tools for cybersecurity intrusions are commercially available.	a. Secure ICS architectures with built-in, end-to-end security are in all of the organization's critical ICSs. b. Each transportation mode has developed best practices for securely connecting ICSs and business networks, where appropriate. c. Asset owners and operators have established secure interfaces between all ICSs and internal and external systems. d. Most operators have received ICS cybersecurity training commensurate with their respective duties and responsibilities. e. Each mode has established formal working relationships with industry, and has promoted the development of COTS tools that provide real-time monitoring for ICS cybersecurity intrusions.
End State:	**Security solutions for legacy systems, new architecture designs, and secured communications systems in the Transportation Sector are readily available and deployed across the Sector.**	

Goal 4: Manage Incidents

	Objectives	Milestones and Metrics
Near-Term (0-2 years)	a. Develop and deploy sensors and systems to detect and report abnormal activity. b. Identify recommended practices and approved guidelines for incident reporting and information sharing of ICS cybersecurity-related events. c. Begin developing and implementing associated continuous improvement mechanisms for incident reporting and Information sharing, and establish a process for disseminating the updated information to stakeholders. d. Develop and incorporate cyber incident response and recovery planning into established business continuity plans. e. Develop procedures for responding to ICS incidents, and provide employees with training on response procedures for ICS incidents commensurate with their roles and responsibilities. f. Work with vendors on specifications for new ICS detection and response tools and equipment.	a. Some asset owners and operators have deployed sensors and systems for detecting and reporting abnormal ICS activity. b. Each organization has identified the practices and guidelines for incident reporting and information sharing it will follow for managing ICS cybersecurity-related events. c. Each organization has begun developing and implementing continuous improvement mechanisms for incident reporting and information sharing, and has established a process for disseminating the updated information to its stakeholders, as appropriate. d. Some asset owners and operators have incorporated a cyber incident response and recovery planning component into their established business continuity plans. e. Most asset owners and operators have developed ICS incident response procedures, and some have provided employees with ICS incident response training commensurate with their roles and responsibilities. f. Many organizations have established formal working relationships with industry for developing specifications for new/improved ICS detection and response tools and equipment.
Mid-Term (2-5 years)	a. Research and implement new, improved, and more effective detection, response, and recovery tools and equipment. b. Establish procedures for the periodic upgrade of business continuity plans and training programs to reflect changes in new tools, equipment, and recommended ICS practices. c. Develop and implement employee training programs that provide specialized instruction on the implementation of new ICS tools and procedures, based on employee roles and responsibilities. d. Develop public communication strategies regarding the potential consequences of transportation network disruption from a cyber incident.	a. Each organization has established a process for identifying, vetting, and implementing, where appropriate, new, improved, and more effective detection, response, and recovery tools and equipment. b. Each organization has established and implemented procedures for periodically updating its business continuity plans and training programs to reflect current ICS detection, response, and recovery tools, equipment, and practices. c. Each organization has developed and implemented employee training programs that provide specialized instruction on the implementation of ICS tools and procedures, and many employees have been trained on these programs, commensurate with their ICS roles and responsibilities. d. Each organization has developed public communication strategies for disseminating the potential transportation network disruption consequences resulting from a cyber incident.
Long-Term (5-10 years)	a. Encourage the widespread implementation and use of automated self-configuring ICS architectures as they become commercially available, in accordance with defined security and safety system priorities. b. Identify and implement real-time detection and response ICS tools and equipment in each mode and throughout the Transportation Sector. c. Research existing ICS cybersecurity certification programs for operators, security, and IT staff, determine which one(s) are best for the organization, and integrate these programs into the organization's overall training/certification program.	a. Self-configuring ICS network architectures are in place in most asset owner/operator facilities, and are in accordance with defined security and safety system priorities. b. Real-time ICS detection and response tools and equipment are present in each mode and throughout the Transportation Sector. c. Many operators, security, and IT staff have successfully completed an ICS cybersecurity certification program that is integrated into the organization's overall training/certification program.

End State: **The Transportation Sector is quickly alerted of cybersecurity ICS incidents, and sophisticated, effective, and efficient mitigation strategies are implemented and in operation.**

8.0 Significant Accomplishments

The Transportation Sector has already implemented a variety of proactive cybersecurity programs and initiatives designed to increase awareness on preventing, identifying, and responding to ICS cybersecurity issues. For example, most of the modes have developed, or are in the process of developing, ICS protection standards and procedures. A listing of these standards, along with their current development status, is provided in Appendix C.

One of the long-term objectives described for Goal 1 (Build a Culture of Cybersecurity) in Section 7.0 of this Roadmap is to “establish Information Sharing and Analysis Centers (ISACs) (or equivalent) for each transportation mode and for the Transportation Sector.” The purpose of ISACs, or their equivalent, is to serve as the conduit for cross-modal lessons learned and best practices in ICS cybersecurity, and to provide a forum for partnership, outreach, and information sharing. The Surface Transportation Mode already has active ISACs for both surface transportation and public transit. In April 2012, the Aviation SCC official formed an information sharing working group; together with DHS, this group has begun working on the creation of an Aviation ISAC.

9.0 Threats, Challenges, and Priorities

9.1 Threats

Cybersecurity threats in the Transportation Sector have the potential to impact ICSs. For example, new generation aircraft and legacy aircraft are designed or retrofitted with technologies such as Ethernet IP-enabled networks, wireless connectivity (e.g., Bluetooth) capabilities, and GPSs. Similarly, trains are now supplied with onboard IT systems that provide and receive real-time updates on track conditions, train position, train separation, car status, and other operational data. While such technologies are designed to provide faster and more reliable communications, these wireless communication advances result in aircraft and trains no longer functioning as closed systems, thus increasing the e-enabled threats and risks to these transportation mediums.

Many pipelines are now supplied with SCADA systems, RTUs, and automated pressure regulators and control valves. If this pipeline infrastructure is intentionally attacked, many control valves and pressure regulators could simultaneously be affected; if thousands of gas pressure regulators were to fail simultaneously throughout the U.S., the widespread outbreak of pressure surges could cause so many simultaneous explosions and fires that state and local emergency response networks would be overwhelmed, and the resulting conflagrations could destroy entire cities.

Today's control systems in the Highway and Maritime Modes are often not only automated but also highly integrated. Interconnected road networks are controlled by numerous systems and devices such as traffic signal systems, ramp metering systems, road weather information systems, and field devices that feed into a traffic management center. Control systems at ports and terminals not only automate access to particular areas but also control container loading and unloading operations. If an individual system or device was deliberately attacked, the potential to affect multiple control systems would be a distinct reality.

9.2 Challenges

In general, challenges to cybersecurity consist not only of the direct risk factors that increase the probability of a successful attack and the severity of the consequences, but also those factors that limit the ability to implement ideal security enhancements. Risk is defined by threat, vulnerability, and consequences.[28] Direct risk challenges include the threat, i.e., those who seek to attack and compromise cyber system; the means of attack, which relies on taking advantage system vulnerabilities; the nature of the system attacked, such as the degree of hazard of the material; the value of the material and systems; and how loss of control can lead to interaction with humans, property, and the environment. Challenges related to the implementation of security measures include organizational, institutional, economic, and technical factors that either limit the availability of security measures, or increase the difficulty of implementing the optimum security enhancements.[29]

---

[28] US Department of Commerce, NIST, *Special Publication 800-30: Risk Management Guide for Information Technology Systems*, July 2002.
[29] Chemical Sector Roadmap Working Group, *Roadmap to Secure Control Systems in the Chemical Sector*, September 2009.

9.3 Priorities

Individual ICSs may have inherently different levels of cybersecurity due to modal differences, organizations' business operations, specific policies followed, etc. Under some circumstances, an organization may decide not to activate an ICS cybersecurity feature, based on the organization's risk management assessment/plan, security considerations, or other reasons. Because transportation modes, as well as individual organizations within each mode, are at different stages of identifying and implementing cybersecurity features, a "one size fits all" approach does not work for addressing cybersecurity in the Transportation Sector. Consequently, each organization, and each mode, should use the Goals, Objective, and Milestones and Metrics to identify the cybersecurity features currently in place and to determine the remaining activities necessary for improving cybersecurity performance.

The WG developed this Transportation Roadmap to be a baseline for guiding the transportation industry toward improving ICS cybersecurity. Because the purpose of this Transportation Roadmap is to develop a general 10-year cybersecurity for ICSs outlook that applies to all modes, specificity within each mode and at the individual organization level is not intended for this first roadmap deliverable. As the Transportation Sector matures in ICS cybersecurity and as each mode grows in its cybersecurity knowledge and practices, the Transportation Roadmap should be updated and refined with these additional layers of specificity, including defining specific challenges inherent in securing transportation ICSs, as well as establishing priorities for cybersecurity activity implementation.

10.0 Implementation[30]

This Transportation Roadmap is a living document; it will continue to evolve as the transportation industry reacts to cyber threats, business pressures, operational constraints, societal demands, and unanticipated events. By working together to develop this Transportation Roadmap, the transportation modes have leveraged a broad range of operational and infrastructure protection experience to identify the most significant ICS challenges within the next 10 years and to develop actions that industry and government can take to begin enhancing cybersecurity in the Transportation Sector.

Implementing this Transportation Roadmap will require the continued collective commitment, collaboration, resources, and efforts of the key transportation stakeholders shown in Figure 16. Strong leadership, action, and persistence are needed to ensure that important issues receive adequate support and resources. In addition, achieving early successes and communicating these achievements to the transportation community are important for maintaining momentum generated by the Transportation Roadmap and convincing asset owners and stakeholders that the control systems security framework outlined in this Transportation Roadmap can work.

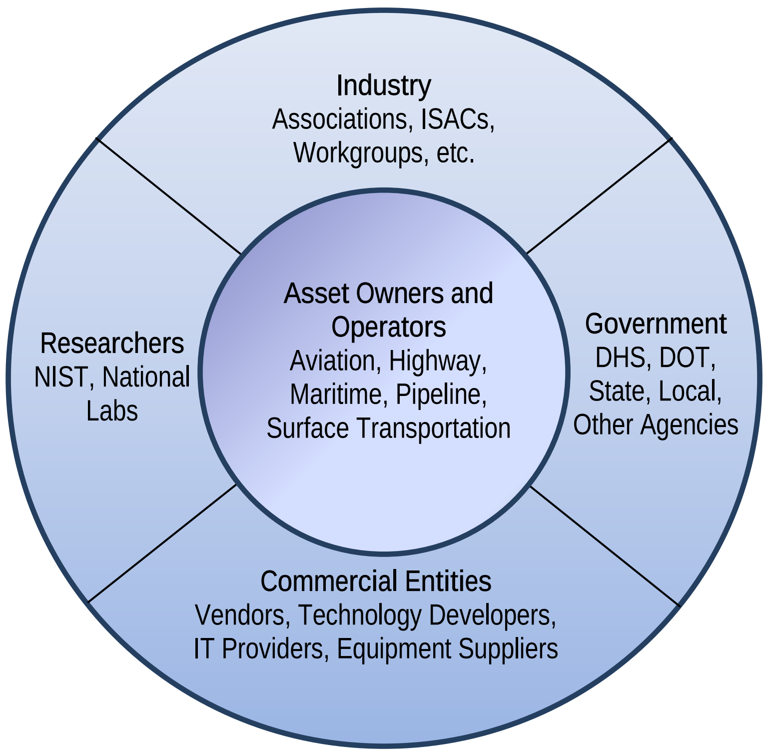

Figure 16: Transportation Stakeholders

---

30 Information from the Water Sector Coordinating Council Cyber Security Working Group, *Roadmap to Secure Control Systems in the Water Sector*, March 2008, October 2008, and October 2009 versions, was used to develop this section.

DHS has identified TSA as the SSA for the Transportation Sector and the USCG as the SSA for the Maritime Mode[31]; as such, these agencies are responsible for identifying, prioritizing, and coordinating the protection of CIKR in the Transportation Sector to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them[32]. The U.S. Department of Transportation (DOT) is changed with assisting the Transportation Sector SSAs in their CIKR protection efforts. While the precise roles of organizations in implementing this roadmap have not yet been determined, they will take shape as this Transportation Roadmap is disseminated and reviewed by those engaged. The contributors to this Transportation Roadmap encourage organizations and individuals to participate in ways that will best capitalize on their distinct skills, capabilities, and resources for developing, refining, and expanding on the potential security solutions and enhancements described in the Metrics and Milestones.

Figure 17 identifies the Transportation Roadmap implementation process.

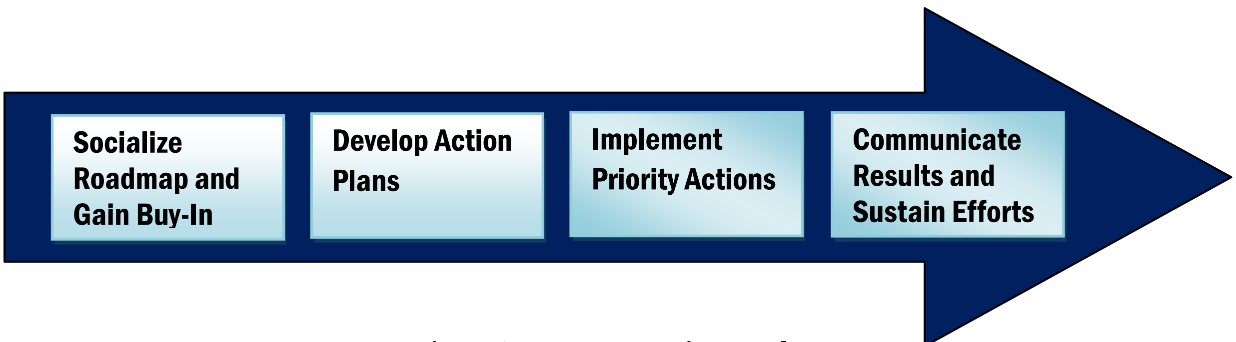

Figure 17: Transportation Roadmap Implementation Process

Socialize Roadmap and Gain Buy-In

While the precise roles of organizations in implementing this Transportation Roadmap have not yet been determined, these roles will take shape as the Transportation Roadmap is disseminated and reviewed by those engaged. The roadmap socialization process should include motivating industry leaders to step forward and initiate the most time-sensitive projects.

Develop Action Plans

Industry and government partners within each transportation mode should collaborate to develop action plans for implementing the Goals and Objectives outlined in this Transportation Roadmap. These action plans should identify a prioritization scheme that reflects those activities deemed most important to protecting the transportation mode's ICS from a cyber attack.

---

[31] DHS, *Transportation Systems, Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan*, May 2007.
[32] HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*. December 17, 2003.

Implement Priority Actions
Each transportation mode, and the Transportation Sector as a whole, should execute cybersecurity plans, assess progress, make necessary adjustments, and deliver tangible results. The Milestones and Metrics provided in this Transportation Roadmap provide modal- and Sector-level benchmarks for identifying whether the Objectives have been achieved.

Communicate Results and Sustain Efforts
Each transportation mode should develop a communication strategy that encourages active stakeholder participation within the mode and informs the Transportation Sector on progress. Where possible, transportation modes should utilize/expand on communication capabilities already in place at ISACs and/or the equivalent.

Appendix A: National Policy Guidance on Cyber Control System Security[33]

In 1988, Presidential Decision Directive NSC-63 (PDD-63), "Critical Infrastructure Protection," was issued recognizing the need for enhanced security of the nation's cyber aspects of critical infrastructure. Although directed specifically to information systems, it recognized the interdependencies within the critical infrastructure sectors and the reliance of that infrastructure on automated, cyber systems. The directive called for voluntary private-public partnerships of the type formalized in the NIPP, provided an assignment of government agencies as lead sector agencies, and called for the creation of private sector ISACs, which evolved into the Sector Information Systems Advisory Councils.

Federal Information Security Management Act of 2002 requires that Federal agencies develop a comprehensive information technology security program to ensure the effectiveness of information security controls over information resources that support Federal operations and assets. This legislation is relevant to the part of the NIPP that governs the protection of Federal assets and the implementation of cyber-protective measures under the critical infrastructure Sector-Specific Plans.

The *Cybersecurity Research and Development Act of 2002* allocates funding to the National Institute of Standards and Technology (NIST) and to the National Science Foundation (NSF) for the purpose of facilitating increased R&D for computer network security and supporting research fellowships and training. This act establishes a means of enhancing basic R&D related to improving the cybersecurity of CIKR.

The *National Strategy for Homeland Security* and the *Homeland Security Act of 2002* responded to the attacks of September 11, 2011 by creating the policy framework for addressing homeland security needs and restructuring government activities, which resulted in the creation of DHS.

In early 2003, the *National Strategy to Secure Cyberspace* outlined priorities for protecting against cyber threats and the damage these threats can cause. It called for DHS and the Department of Energy (DOE) to work in partnership with industry to "... develop best practices and new technology to increase security of digital control systems/SCADA systems, to determine the most critical digital control systems/SCADA-related sites, and to develop a prioritized plan for short-term cybersecurity improvements in those sites."

[33] Information from the Industrial Control Systems Cross-Sector Roadmap Working Group, *Cross-Sector Roadmap for Cybersecurity of Control Systems*, September 30. 2011, was used to develop this section.

Appendix A: National Policy Guidance on Cyber Control System Security (continued)

In late 2003, the President issued Homeland Security Presidential Decision 7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," to implement Federal policies. HSPD-7 outlined how government will coordinate critical infrastructure protection and assigned DOE the task of working with the Energy Sector to improve physical and cybersecurity in conjunction with DHS. Responsibilities include collaborating with all government agencies and the private sector, facilitating vulnerability assessments of the sector, and encouraging risk management strategies to protect against and mitigate the effects of attacks. HSPD-7 also called for a national plan to implement critical infrastructure protection.

Executive Order (EO) 13231 (as amended by EO 13286 of February 28, 2003 and EO 13385 of September 29, 2005) established the National Infrastructure Advisory Council (NIAC) as the President's principal advisory panel on critical infrastructure protection issues spanning all sectors. The NIAC is composed of not more than 30 President-appointed members, who are selected from the private sector, academia, and state and local government, and represent senior executive leadership expertise from the CIKR as delineated in HSPD-7. The NIAC provides the President, through the Secretary of Homeland Security, with advice on the security—both physical and cyber—of critical infrastructure. The NIAC is charged with improving the cooperation and partnership between the public and private sectors in securing critical infrastructure, and advises on policies and strategies for risk assessment and management, information sharing, and protective strategies and provides clarification on roles and responsibilities between public and private sectors.

Appendix B: Roadmap Process

DHS CSSP and DOT's John A. Volpe National Transportation Systems Center (Volpe Center) signed a Statement of Work agreement in 2011, with one of the major tasks being the development of a roadmap for cybersecurity of control systems in the Transportation Sector (Transportation Roadmap). The Transportation Roadmap specifications were:

- Build upon previous CIKR roadmaps developed to address control systems,
- Utilize key methodology information developed during the creation of the *Cross-Sector Roadmap for Cybersecurity of Control Systems*, and
- Provide a ten-year, high-level outlook and framework for all transportation modes (Aviation, Highway, Maritime, Pipeline, and Surface Transportation—including Freight Rail and Passenger Rail/Public Transit) in the form of cybersecurity control systems goals and milestones.

From March to July 2011, the Volpe Center Roadmap Task Lead conducted a review of the following CIKR roadmaps that were available at the time of the review:

- *Roadmap to Secure Control Systems in the Chemical Sector* (September 2009)
- *Roadmap to Secure Control Systems in the Energy Sector* (January 2006)
- *Roadmap to Secure Control Systems in the Water Sector* (March 2008, October 2008, and October 2009 versions)

In addition, the Volpe Center Transportation Roadmap Task Lead reviewed the *Cross-Sector Roadmap for Cybersecurity of Control Systems* (multiple draft versions, 2011). This roadmap was developed as a guide for CIKR to use to develop sector-specific roadmaps.

The Volpe Center Transportation Roadmap Task Lead compared the four roadmaps; identified the sections and content common to all; identified different sections where similar information was presented; and found common intents among the goals and objectives. These activities culminated in the development of a draft Transportation Roadmap outline and draft Goals, Objectives, Metrics, and Milestones in August 2011.

The Volpe Center Transportation Roadmap Task Lead attended the May 2011 ICSJWG Conference, and participated in the Cross-Sector Roadmap WG meeting held during the conference. Contacts made and information discussed at the meeting provided addition context for developing the Transportation Roadmap.

Appendix B: Roadmap Process (continued)

In July 2011, modal industry and government representatives were invited to participate in a Transportation Roadmap Working Group (WG). Monthly WG teleconference meetings began in August 2011. Because the Goals, Objectives, Metrics, and Milestones information contains the ten-year outlook activities designed to improve transportation control systems cybersecurity, the WG decided to focus its initial efforts on developing this information. From August 2011 to March 2012, the Transportation Roadmap WG reviewed, edited, and added information to the Goals, Objectives, Metrics, and Milestones information, ensuring that the information was applicable to all modes. In April and May 2012, the WG reviewed and developed information for the remaining Transportation Roadmap sections.

The draft Transportation Roadmap was submitted to DHS CSSP for first-level review (initial draft) on May 31, 2012 and for second-level review (final draft) on July 20, 2012.

Appendix C: Transportation Cybersecurity Standards

Mode	Organization	Title	Summary and Additional Information	Status
Aviation	FAA	Information Security Certification and Accreditation (C&A) Handbook	The primary source of procedures and guidance that supports the C&A process in protecting the confidentiality, integrity, and availability of FAA's information that is collected, processed, transmitted, stored, or disseminated in its general support systems, major applications, ICSs, and other applications.	Published
Aviation	RTCA	Airworthiness Security Methods and Considerations	This document is a resource for certification authorities and the aviation industry for developing or modifying aircraft systems and equipment when there is the possibility of danger to flight from volitional human action involving information or information system interfaces. It presents permissible methodologies to meet the data requirements and compliance objectives of an airworthiness security process.	Private Draft
Aviation	RTCA	Airworthiness Security Process Specification	The first of a series of documents on aeronautical systems security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment. This document addresses only aircraft type certification and is not yet widely implemented, but is derived from understood best practices.	Private Draft
Aviation	AEEC	Guidelines for the Incorporation of Cyber Security in the Development of AEEC Documents	This Technical Application Bulletin represents the current (2009) cyber security thinking and experience useful in the development of further AEEC specifications. The intent is to periodically update the cyber security guidelines and disseminate them to AEEC Subcommittees as conditions warrant.	Under Review
Aviation	ARINC	ARINC Project Paper 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	The purpose of this document is to facilitate an understanding of aircraft information security and to develop aircraft information security operational concepts. This document also provides an aircraft information security process framework relating to airline operational needs that, when implemented by an airline and its suppliers, will enable the safe and secure dispatch of the aircraft in a timely manner. This framework facilitates development of cost-effective aircraft information security and provides a common language for understanding security needs.	Private Draft

Appendix C: Transportation Cybersecurity Standards (continued)

Maritime	USCG	Command, Control, Communication, Computers and Information Technology (C4IT) Strategic Plan	This plan is intended to be used by the USCG and C4IT community to establish and prioritize recommendations for implementing improvements to the USCG's C4IT infrastructure, systems, applications, products, policies, practices, and processes. The document focuses on activities that must occur in the next five years to begin achieving DHS's and USCG's long-term goals.	Published
Pipeline	INGAA	Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry	This document provides guidance on addressing the control system cybersecurity plans section of the natural gas pipeline operators' TSA-required corporate security program. It provides a set of guidelines to assist operators of natural gas pipelines in managing their control systems cyber security requirements, and sets forth details of the unique risk and impact-based differences between the natural gas pipeline industry and the hazardous liquid pipeline and liquefied natural gas operations.	Published
Pipeline	API	API Standard 1164: Pipeline SCADA Security (Second Edition)	This standard on SCADA security provides guidance to the operators of oil and gas liquid pipeline systems for managing SCADA system integrity and security. The use of this document has applicability beyond pipelines regulated under Title 49 CFR 195.1, and should be viewed as a listing of best practices to be employed when reviewing and developing standards for a SCADA system.	Public Draft
Pipeline	TSA	Pipeline Security Guidelines	These guidelines are applicable to natural gas and hazardous liquid transmission pipelines, natural gas distribution pipelines, and liquefied natural gas facility operators. They also apply to pipeline systems that transport materials categorized as toxic inhalation hazards.	Published
Surface Transportation	APTA	Securing Control and Communications Systems in Transit Environments, Parts 1 and 2	This document addresses the security of the following passenger rail and/or bus systems: SCADA, traction power control, emergency ventilation control, alarms and indications, fire/intrusion detection systems, train control/signaling, fare collection, automatic vehicle location, physical security feeds (CCTV, access control), public information systems, public address systems, and radio/wireless/related communication. In the event that security/safety or other standards exist for any of the above systems, this Recommended Practice will supplement, provide additional guidance for, or provide guidance on how control systems may securely interface with these systems.	Published (Part 1) Final Draft (Part 2)